PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2006-033729
(43)Date of publication of application : 02.02.2006

(51)Int.Cl. *H04L 9/32 (2006.01)*
H04L 9/10 (2006.01)

(21)Application number : 2004-213193
(22)Date of filing : 21.07.2004

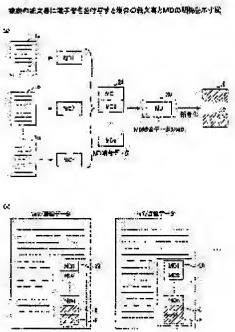
(71)Applicant : RICOH CO LTD
(72)Inventor : OTA YUSUKE

(54) DOCUMENT COMPUTERIZATION METHOD, DOCUMENT COMPUTERIZING APPARATUS AND DOCUMENT COMPUTERIZING PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a document computerization method, document computerizing apparatus and document computerizing program which enable a processing time of encryption processing to be shortened when an electronic signature is imparted to image data of a document.

SOLUTION: The document computerization method is provided by which an electronic signature generated by an information processing terminal is imparted to image data of optically read one or more documents, wherein the method includes: a first MD generation step of generating a first message digest of the image data for each document; an MD coupling data generation step of generating MD coupling data by coupling a plurality of first message digests generated by the first MD generation step; a second MD generation step of generating a second message digest of the MD coupling data generated by the MD coupling data generation step; a terminal encryption step of encrypting the second message digest generated by the second MD generation step using an encryption key of the information processing terminal; and a first attachment step of attaching the second message digest encrypted by the terminal encryption step to each of image data together with the MD coupling data.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-33729
(P2006-33729A)
(43)公開日　平成18年2月2日(2006.2.2)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	675B	5J104
H04L	9/10	(2006.01)	H04L	9/00	621A	

審査請求 未請求　請求項の数 11　OL　（全 13 頁）

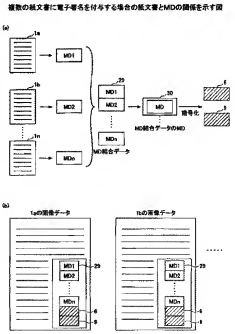
(21)出願番号　特願2004-213193 (P2004-213193)
(22)出願日　平成16年7月21日 (2004.7.21)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　太田　雄介
東京都大田区中馬込１丁目３番６号　株式会社リコー内

Fターム(参考)　5J104 AA18　EA22　LA05　LA06　PA14

(54)【発明の名称】文書電子化方法、文書電子化装置及び文書電子化プログラム

(57)【要約】
【課題】　文書の画像データに電子署名を付与する場合に、暗号化処理の処理時間を低減することが可能な文書電子化方法、文書電子化装置及び文書電子化プログラムを提供すること。
【解決手段】　光学的に読み取った１以上の文書の画像データに、情報処理端末により生成した電子署名を付与する文書電子化方法において、文書毎に画像データの第１のメッセージダイジェストを生成する第１のMD生成ステップと、第１のMD生成ステップにより生成された複数の第１のメッセージダイジェストを結合してMD結合データを生成するMD結合データ生成ステップと、MD結合データ生成ステップにより生成されたMD結合データの第２のメッセージダイジェストを生成する第２のMD生成ステップと、第２のMD生成ステップにより生成された第２のメッセージダイジェストを情報処理端末の暗号鍵により暗号化する端末暗号化ステップと、端末暗号化ステップにより暗号化された第２のメッセージダイジェストを、MD結合データと共に、各画像データに添付する第１の添付ステップと、を有することを特徴と



【特許請求の範囲】
【請求項1】
光学的に読み取った１以上の文書の画像データに、情報処理端末により生成した電子署名を付与する文書電子化方法において、
文書毎に前記画像データの第１のメッセージダイジェストを生成する第１のMD生成ステップと、
前記第１のMD生成ステップにより生成された複数の第１のメッセージダイジェストを結合してMD結合データを生成するMD結合データ生成ステップと、
前記MD結合データ生成ステップにより生成された前記MD結合データの第２のメッセージダイジェストを生成する第２のMD生成ステップと、
前記第２のMD生成ステップにより生成された第２のメッセージダイジェストを前記情報処理端末の暗号鍵により暗号化する端末暗号化ステップと、
前記端末暗号化ステップにより暗号化された第２のメッセージダイジェストを、前記MD結合データと共に、各画像データに添付する第１の添付ステップと、
を有することを特徴とする文書電子化方法。
【請求項2】
前記第２のMD生成ステップにより生成された第２のメッセージダイジェストを、前記画像データを生成した画像データ生成装置の暗号鍵により暗号化する装置暗号化ステップと、
前記装置暗号化ステップにより暗号化された第２のメッセージダイジェストを、各画像データに添付する第２の添付ステップと、
を有することを特徴とする請求項１記載の文書電子化方法。
【請求項3】
前記第１のMD生成ステップは、前記文書のページ数情報に基づき、文書毎の画像データの第１のメッセージダイジェストを生成する、
ことを特徴とする請求項１記載の文書電子化方法。
【請求項4】
前記第１のMD生成ステップは、所定の画像データに基づき、文書毎の画像データの第１のメッセージダイジェストを生成する、
ことを特徴とする請求項１記載の文書電子化方法。
【請求項5】
前記情報処理端末は、ＩＣカードであることを特徴とする請求項１記載の文書電子化方法。
【請求項6】
光学的に読み取った１以上の文書の画像データに、情報処理端末により生成した電子署名を付与する文書電子化装置において、
文書毎に前記画像データの第１のメッセージダイジェストを生成する第１のMD生成手段と、
前記第１のMD生成手段により生成された複数の第１のメッセージダイジェストを結合してMD結合データを生成するMD結合データ生成手段と、
前記MD結合データ生成手段により生成された前記MD結合データの第２のメッセージダイジェストを生成する第２のMD生成手段と、
前記第２のMD生成手段により生成された第２のメッセージダイジェストを前記情報処理端末の暗号鍵により暗号化する端末暗号化手段と、
前記端末暗号化手段により暗号化された第２のメッセージダイジェストを、前記MD結合データと共に、各画像データに添付する第１の添付手段と、
を有することを特徴とする文書電子化装置。
【請求項7】
前記第２のMD生成手段により生成された第２のメッセージダイジェストを、前記画像

データを生成した画像データ生成装置の暗号鍵により暗号化する装置暗号化手段と、
　前記装置暗号化手段により暗号化された第２のメッセージダイジェストを、各画像データに添付する第２の添付手段と、
　を有することを特徴とする請求項６記載の文書電子化装置。
【請求項８】
　前記第１のＭＤ生成手段は、前記文書のページ数情報に基づき、文書毎の画像データの第１のメッセージダイジェストを生成する、
　ことを特徴とする請求項６記載の文書電子化装置。
【請求項９】
　前記第１のＭＤ生成手段は、所定の画像データに基づき、文書毎の画像データの第１のメッセージダイジェストを生成する、
　ことを特徴とする請求項６記載の文書電子化装置。
【請求項10】
　前記情報処理端末は、ＩＣカードであることを特徴とする請求項６記載の文書電子化装置。
【請求項11】
　請求項１ないし５記載の文書電子化方法をコンピュータに実行させる文書電子化プログラム。
【発明の詳細な説明】
【技術分野】
【0001】
　本発明は、文書を電子化して署名し得る文書電子化方法、文書電子化装置及び文書電子化プログラムに関し、特に、電子署名に係る暗号化処理の処理量を低減することが可能な文書電子化方法、文書電子化装置及び文書電子化プログラムに関する。
【背景技術】
【0002】
　高度情報化が進展するにつれ、従来は紙で保存が義務付けられていた書類を、電子的に保存できるようにすることが求められている。しかしながら、電子文書はデジタルデータであることから、痕跡を残さない改ざんが可能である。このため、電子的に保存された文書を、原本と同等に取り扱うことは認められていなかった。
【0003】
　紙文書の原本を電子文書で保存し、その電子文書を原本とするためには、電子文書が原本の紙文書と同じ内容であることを保証しなくてはならない。係る要請に対し、画像形成装置により電子化した画像情報にユーザの保持する暗号鍵を用いて電子署名を施す画像形成装置が提案されている（例えば、特許文献１参照。）。
【0004】
　特許文献１の画像形成装置では、まず、紙文書をスキャンして得られた電子文書のメッセージダイジェストを生成する。画像形成装置は、ユーザの管理する暗号鍵をユーザのＵＳＢトークンから取得してメッセージダイジェストを暗号化し、暗号化されたメッセージダイジェストを電子文書に合成する。これにより、当該電子文書はユーザにより電子署名が施されたことが推定される。
【特許文献1】特開２００３－２２４７２８号公報
【発明の開示】
【発明が解決しようとする課題】
【0005】
　しかしながら、ＵＳＢトークンから暗号鍵を取得した画像形成装置がメッセージダイジェストを暗号化するのでは、暗号鍵が画像形成装置に残存し、第三者が盗み見る可能性が存在する。また、暗号鍵を記憶したＵＳＢトークン等を、ユーザの責任で管理するため、紛失、盗難、漏洩等のおそれがあった。第三者がＵＳＢメモリ等を入手して暗号化する場合には、電子署名の信頼性が失われるという問題が生じる。
【0006】

これに対し、ＩＣカードによりメッセージダイジェストの暗号化を行うことが考えられる。ＩＣカードであれば、個人認証機能を有するため、第三者が利用することは困難であるし、また、ＩＣカードは耐タンパ性を有するので、暗号鍵を取り出すことは困難である。したがって、ＩＣカードが暗号化処理を行い、暗号化処理により得られた電子署名を電子文書に付与することで、第三者のなりすましを防止して、電子文書が原本と同じであることを保証できる。

【0007】

しかしながら、ＩＣカードが搭載するＣＰＵの処理能力はそれほど高くないため、暗号化処理の高速化が困難である。特に、複数の独立した紙文書に電子署名を付与する場合などでは、スキャニングは終了しているのに、ＩＣカードによる暗号化処理に時間が費やされるという問題がある。特にＡＤＦ（Ａｕｔｏ Ｄｏｃｕｍｅｎｔ Ｆｅｅｄｅｒ）を有する画像形成装置や法務部など、複数の文書に連続して電子署名を付与する場合には、ユーザの待機時間が増大する。

【0008】

本発明は、上記問題に鑑み、文書の画像データに電子署名を付与する場合に、暗号化処理の処理時間を低減することが可能な文書電子化方法、文書電子化装置及び文書電子化プログラムを提供することを目的とする。

【課題を解決するための手段】

【0009】

上記課題を解決するため、本発明は、光学的に読み取った１以上の文書の画像データに、情報処理端末により生成した電子署名を付与する文書電子化方法において、文書毎に画像データの第１のメッセージダイジェストを生成する第１のＭＤ生成ステップと、第１のＭＤ生成ステップにより生成された複数の第１のメッセージダイジェストを結合してＭＤ結合データを生成するＭＤ結合データ生成ステップと、ＭＤ結合データ生成ステップにより生成されたＭＤ結合データの第２のメッセージダイジェストを生成する第２のＭＤ生成ステップと、第２のＭＤ生成ステップにより生成された第２のメッセージダイジェストを情報処理端末の暗号鍵により暗号化する端末暗号化ステップと、端末暗号化ステップにより暗号化された第２のメッセージダイジェストを、ＭＤ結合データと共に、各画像データに添付する第１の添付ステップと、を有することを特徴とする。

【0010】

本発明によれば、文書の画像データに電子署名を付与する場合に、暗号化処理の処理時間を低減することが可能な文書電子化方法を提供することができる。

【0011】

また、本発明の文書電子化方法において、第２のＭＤ生成ステップにより生成された第２のメッセージダイジェストを、画像データを生成した画像データ生成装置の暗号鍵により暗号化する装置暗号化ステップと、装置暗号化ステップにより暗号化された第２のメッセージダイジェストを、各画像データに添付する第２の添付ステップと、を有することを特徴とする。画像データ生成装置の暗号鍵により第２のメッセージダイジェストを暗号化することで、電子化後に画像データが改ざんされていないことが検証できる。また、ユーザ固有の電子署名を付与することから、責任の所在が明確になるため、紙文書を改ざんしてからスキャンすることを抑止できる。

【0012】

また、本発明の文書電子化方法において、第１のＭＤ生成ステップは、文書のページ数情報に基づき、文書毎の画像データの第１のメッセージダイジェストを生成する、ことを特徴とする。本発明によれば、例えばユーザにより予め入力された、複数の文書がそれぞれ有するページ数情報に基づき、文書間の区切りを検出して第１のメッセージダイジェストを生成できる。したがって、ページ数の同じ複数の文書をＡＤＦ等で一度に画像データとするような場合に、文書毎に第１のメッセージダイジェストを生成できる。

【0013】

また、本発明の文書電子化方法において、第１のＭＤ生成ステップは、所定の画像デー

タに基づき、文書毎の画像データの第１のメッセージダイジェストを生成する、ことを特徴とする。所定の画像データとは、例えば、所定の一色のみの画像データのように、スキャンした文書の画像データと区別しうる画像データをいう。したがって、本発明では、文書間に予め所定の区切り用紙が挟まれていることが好適である。本発明によれば、ページ数の異なる複数の文書をＡＤＦ等で一度に画像データとするような場合に、文書毎に第１のメッセージダイジェストを生成できる。

【0014】

また、本発明の文書電子化方法において、情報処理端末は、ＩＣカードであることを特徴とする。ＩＣカードであれば、暗号鍵を外部から参照できないので、電子署名のセキュリティレベルを向上できる。また、ＩＣカードは、スマートカードと呼ばれるものであってもよいし、特にＣＰＵを搭載しており暗号処理や利用者認証を行うことができれば、携帯電話やＰＤＡ（Ｐｅｒｓｏｎａｌ Ｄａｔａ Ａｓｓｉｓｔａｎｔ）等でもよい。

【0015】

また、上記課題を解決するため、本発明は、光学的に読み取った１以上の文書の画像データに、情報処理端末により生成した電子署名を付与する文書電子化装置において、文書毎に画像データの第１のメッセージダイジェストを生成する第１のＭＤ生成手段と、第１のＭＤ生成手段により生成された複数の第１のメッセージダイジェストを結合してＭＤ結合データを生成するＭＤ結合データ生成手段と、ＭＤ結合データ生成手段により生成されたＭＤ結合データの第２のメッセージダイジェストを生成する第２のＭＤ生成手段と、第２のＭＤ生成手段により生成された第２のメッセージダイジェストを情報処理端末の暗号鍵により暗号化する端末暗号化手段と、端末暗号化手段により暗号化された第２のメッセージダイジェストを、ＭＤ結合データと共に、各画像データに添付する第１の添付手段と、を有することを特徴とする。

【0016】

本発明によれば、文書の画像データに電子署名を付与する場合に、暗号化処理の処理時間を低減することが可能な文書電子化装置を提供することができる。

【0017】

また、本発明の文書電子化装置において、第２のＭＤ生成手段により生成された第２のメッセージダイジェストを、画像データを生成した画像データ生成装置の暗号鍵により暗号化する装置暗号化手段と、装置暗号化手段により暗号化された第２のメッセージダイジェストを、各画像データに添付する第２の添付手段と、を有することを特徴とする。

【0018】

また、本発明の文書電子化装置において、第１のＭＤ生成手段は、文書のページ数情報に基づき、文書毎の画像データの第１のメッセージダイジェストを生成する、ことを特徴とする。

【0019】

また、本発明の文書電子化装置において、第１のＭＤ生成手段は、所定の画像データに基づき、文書毎の画像データの第１のメッセージダイジェストを生成する、ことを特徴とする。

【0020】

また、本発明の文書電子化装置において、情報処理端末は、ＩＣカードであることを特徴とする。

【0021】

また、上記課題を解決するため、本発明は、請求項１ないし５記載の文書電子化方法をコンピュータに実行させる文書電子化プログラムを提供する。

【発明の効果】

【0022】

文書の画像データに電子署名を付与する場合に、暗号化処理の処理時間を低減することが可能な文書電子化方法、文書電子化装置及び文書電子化プログラムを提供することができる。

【発明を実施するための最良の形態】
【0023】
以下、本発明を実施するための最良の形態について、図面を参照しながら実施例を上げて説明する。まず、本実施の形態における、電子署名を付与する方法について概略を説明する。図１は、スキャンした紙文書に電子署名を付与する処理の流れを示す。なお、図１では、特許請求の範囲に記載した情報処理端末をＩＣカードとして記載した。
【0024】
始めに、スキャナ装置のコンタクトガラスの紙文書１がスキャン手段２によりスキャンされ、電子文書３が生成される。
【0025】
次いで、機器署名手段４は、スキャン手段２により電子化された電子文書３に、当該スキャナ装置による機器署名６を付与する。機器署名手段４による機器署名６は、当該署名が当該スキャナ装置より付与されたことを示すもので、当該スキャナ装置固有の秘密鍵を用いて付与される。機器署名手段４は、ハッシュ関数を用いて生成された電子文書３のメッセージダイジェスト（以下、ＭＤと称す）を、スキャナ装置の秘密鍵で暗号化する。機器署名６により、スキャナ装置で電子化した電子文書を修正するような改ざんがあっても、判別することが可能となる。
【0026】
次いで、責任者署名機能４は、電子文書３のＭＤを、ユーザの保持するＩＣカード８に送信する。ＩＣカード８は、搭載されたＣＰＵでＩＣカード８固有の秘密鍵で暗号化し責任者署名９を生成して、スキャナ装置に送信する。責任者署名機能４は、電子文書３に責任者署名９を添付する。以上で、電子文書３に、機器署名６及び責任者署名９が付与された。
【0027】
責任者署名は、スキャン操作を行った者を特定し、所定の権限ある者によりスキャンされたことを示す。機器署名６だけでは、例えば悪意を持った者が紙文書に修正を加えて電子化する可能性が残されるが、責任者署名を付与することで、当該電子文書が権限のある者又は部署により電子化されたことが保証される。機器署名６及び責任者署名９が付与された電子文書３は、署名済みの電子文書を記憶する所定の記憶装置１１に記憶される。
【0028】
続いて、本発明の実施の形態を文書電子化装置を用いて詳細に説明する。図２は、文書電子化装置の機能ブロック図を示す。なお、図２において図１と同一構成部分には同一の符号を付す。
【0029】
文書電子化装置は、ユーザに操作を促すメッセージ等を表示したりユーザからの操作入力を受け付ける情報表示・入力手段２２を有する。情報表示・入力手段２２は、例えばタッチパネルなどで構成され、情報表示・入力手段２２を介して、スキャン条件の設定、スキャンの実行等が行われる。また、情報表示・入力手段２２から、ユーザのＰＩＮ（Ｐｅｒｓｏｎａｌ Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ Ｎｕｍｂｅｒ）が入力される。情報表示・入力手段２２は、入力されたＰＩＮを用いて、カード入出力手段２３に挿入されたＩＣカード８に予め保存されているＰＩＮとの整合性を検証する。ＰＩＮの代わりにバイオメトリクス（顔、音声、 虹採、指紋等）等を用いてもよい。
【0030】
ユーザによりスキャンの実行が指示されると、スキャン手段２が紙文書１を画像データに変換する。スキャン手段２は、紙上の濃淡情報を光学的手法により読み取り、紙文書をデジタルデータにより構成される画像データに変換する。電子化された画像データは、その後の利用のために、例えば、JPEG（Joint Photographic Coding Experts Group）やTIF F（Tagged Image File Format）、PDF（Portable Document Format）といった一般的な画像フォーマットで保存される。画像データは、データ保存手段２４に記憶される。
【0031】

データ保存手段２４は、保存された画像データに対しハッシュ関数によるMDを生成し、該MDを機器署名手段４及び責任者署名手段７に出力する。なお、より詳細には、データ保存手段２４は、第１のMD生成手段、第２のMD生成手段及びMD結合データ生成手段を有し、これらがMDの生成、複数のMDの結合を行う。複数のMDの結合については後述する。

【0032】

機器署名手段４は、データ保存手段２４から入力されたMDを、文書電子化装置が機器内に保持する暗号鍵（秘密鍵）を用い暗号化する。暗号化されたMDは機器による電子署名（機器署名６）として、MDを生成した画像データに対応づけて、又は添付して、データ保存手段２４に記憶される。なお、画像データが改ざんされていないことを後に検証できるように、公開鍵及び公開鍵証明書も一緒に添付しておくことが好適である。また、より詳細には、機器署名手段４は、装置暗号化手段と第２の添付手段を有し、これらが暗号化処理及び画像データへの添付を行う。

【0033】

責任者署名機能７は、データ保存手段２４から入力されたMDを、カード入出力手段２３を介してＩＣカード８に送信する。送信の際には、責任者署名手段７は、ＩＳＯ／ＩＥＣ７８１６で定めるＥｎｃｉｐｈｅｒコマンドを利用することが好適である。ＩＣカード８はこのコマンドを受け、MDを該ＩＣカードが保持する暗号鍵で暗号化し、責任者署名手段７に返す。これにより、ＩＣカードの暗号鍵は外部から参照されないで、ＩＣカードの暗号鍵により暗号化されたMDが生成される。暗号化されたMDはＩＣカード８による電子署名（責任者署名９）として、電子署名を生成した画像データに対応づけて、又は添付して、データ保存手段２４に記憶される。なお、画像データが、権限のある者により暗号化されていることを、後に確認するためにＩＣカード８の公開鍵及び公開鍵証明書も一緒に添付しておくことが好適である。また、より詳細には、責任者署名手段７は、端末暗号化手段、第１の添付手段を有し、これらが暗号化処理及び画像データへの添付を行う。

【0034】

保存データ配信手段２５は、データ保存手段２４に保存された電子署名付き画像データを外部の記憶装置１１に配信する。配信は、データ保存手段２４に責任者の電子署名が付与された画像データが保存されたら順次行ってもよいし、文書電子化装置が使用されていない状態のときに行われてもよい。また、記憶装置１１からの配信要求があった場合に、配信してもよい。なお、記憶装置１１は、例えばネットワークを介して接続されたファイルサーバ等であり、権限のない者のアクセスや画像データの消去等が防止された画像データの長期保存に適した記憶装置１１であることが好適である。

【0035】

また、機器署名手段４、データ保存手段２４、責任者署名手段７を文書電子化装置のコンピュータに実行させる紙文書電子化プログラムは、記録媒体１０に記憶されて配布することができる。本実施形態では、紙文書電子化プログラムは、予め文書電子化装置にインストールされている。紙文書電子署名プログラムは、不図示のプログラムサーバからネットワークを介してダウンロードされてもよい。

【0036】

続いて、図２の文書電子化装置を用いて、複数の紙文書に電子署名を付与する場合について説明する。図３（ａ）は、複数の紙文書に電子署名を付与する場合の紙文書とMDの関係を示す。複数の紙文書１ａ～１ｎは、それぞれが独立した紙文書であり、電子化されても紙文書と同一であることを保証するため、それぞれに電子署名が付与される。データ保存手段２４は、紙文書１ａの画像データが入力されると紙文書１ａのメッセージダイジェストであるMD１を、紙文書１ｂの画像データが入力されると紙文書１ｂのメッセージダイジェストであるMD２を、それぞれ生成する。例えばＡＤＦにセットされた、紙文書が全て画像データに変換され、全ての画像データのMDが生成されると、MD結合データ生成手段は、それらMD１～MDｎのMDを結合し、MD結合データ２９を生成する。次いで、データ保存手段２４は、更にMD結合データ２９のMD３０を生成する。

【0037】
データ保存手段２４は、ＭＤ３０を機器署名手段４及び責任者署名手段７に出力する。機器署名手段４は、データ保存手段２４から入力されたＭＤ３０を、文書電子化装置が機器内に保持する暗号鍵（秘密鍵）を用いて暗号化し、機器署名６を生成する。
【0038】
また、責任者署名手段７は、データ保存手段２４から入力されたＭＤ３０を、カード入出力手段２３を介してＩＣカード８に送信する。ＩＣカード８は、ＭＤ３０を、該ＩＣカードが保持する暗号鍵で暗号化し、責任者署名９を生成する。生成された機器署名６と責任者署名９は、図３（ｂ）に示すように、ＭＤ結合データ２９と共に紙文書１ａ等の画像データに添付される。
【0039】
したがって、本実施の形態では、独立した複数の紙文書に電子署名を付与する場合において、ＩＣカード８による暗号化処理が１回で終了する。通常、ＩＣカードの暗号化処理能力は低いので、複数の紙文書に電子署名を付与する場合、紙文書毎に暗号化処理を行っていたのでは、暗号化処理に時間が費やされる。この場合、紙文書の画像データ化が終了しても、ＩＣカードが文書電子化装置に使用されているので、ユーザは、文書電子化装置を離れることができないが、本実施の形態のように、ＭＤ結合データのＭＤを暗号化することで、紙文書の数に関わらず１回の暗号化処理で電子署名を生成できる。
【0040】
また、電子署名を検証する場合、機器署名６・責任者署名９とＭＤ結合データ２９を、共に画像データに添付して保存してあるので、画像データのいずれかが改ざんされた場合も、改ざんされた画像データを特定できる。すなわち、検証者は、文書電子化装置の公開鍵により機器署名６を復号化しＭＤ３０を、又は／及び、ＩＣカード８の公開鍵により責任者署名９を復号化してＭＤ３０を、それぞれ生成する。また、画像データ（例えば１ａ）に添付されたＭＤ結合データ２９から、ハッシュ関数を利用してＭＤ３０を生成する。復号化されたＭＤ３０とハッシュ関数により求めたＭＤ３０を比較することで、まず、ＭＤ結合データ２９を検証できる。
【0041】
また、紙文書１ａの画像データからハッシュ関数を利用してＭＤ１を生成し、該ＭＤ１をＭＤ結合データ２９のＭＤ１と比較することで、紙文書１ａの画像データを検証できる。他の画像データについても同様の処理を行うことで、改ざんされた画像データを特定できる。
【0042】
したがって、本実施の形態の文書電子化装置では、複数の紙文書毎に検証可能な電子署名を付与する場合に、暗号化処理の処理量を低減できる。なお、文書電子化装置は充分な処理装置を有していることが多いので、機器署名６のように１回だけ暗号化を行うのではなく、各画像データについて機器署名手段４が機器署名をしてもよい。
【実施例】
【0043】
複数の紙文書毎に検証可能な電子署名を付与する文書電子化装置における処理の実施例を説明する。図４は、スキャンされた複数の紙文書に電子署名を付与する処理のシーケンス図を示す。
【0044】
ユーザは、紙文書をＡＤＦ等にセットしスキャンの実行を指示する（Ｓ１）。その際、紙文書が複数ある場合の、複数の紙文書間の区切りに関し設定等を行う。
【0045】
紙文書間の区切りについて説明する。上記した実施の形態では、各紙文書は、１ページであるものとして説明したが、実際には、例えば2ページずつからなる10文書（計20枚）をスキャンして10個の電子文書に対し電子署名を付与する、といったようなケースも考えられる。また、例えば3ページ、20ページ、1ページの3文書に対し電子署名を付与する、

というようなケースも考えられる。このような場合、次のような方法で紙文書間の区切りを検出する。

【0046】

ａ）単位ページ数をあらかじめ文書電子化装置に指示しておく方法。特に、同じページ数の紙文書を複数スキャンする場合に有効となる。図５（ａ）及び（ｂ）は、情報表示・入力手段２２に表示された、各紙文書のページ数を入力する表示画面を示す。同じページ数の紙文書を複数スキャンする場合には、図５（ａ）のように、部数とページ数を入力するだけで、紙文書間の区切りを入力できる。また、各紙文書のページ数が異なる場合には、図５（ｂ）のように、各紙文書毎にページ数を入力することができる。

【0047】

ｂ）文書間の区切りに、文書の区切りを示す特殊な紙（以下、区切り用紙という）を挟み、スキャン手段２が区切り用紙を判別して紙文書間の区切りを検出する方法。多様な紙文書に一度に電子署名する場合に対応できる。図６は、紙文書間の区切りに区切り用紙を挟んだ複数の紙文書の一例を示す。図６のように、スキャン手段２が区切り用紙３５を検出することで、文書電子化装置が紙文書を区切ることができる。

【0048】

なお、区切り用紙３５は、スキャン手段２が、「区切りを示す用紙」であることを認識できる用紙であればよい。例えば、全面黒い紙を区切り用紙としておき、明暗の階調が２５６段階で評価される場合に、スキャン結果の画像データの９５％以上が５階調未満であれば区切りとみなす、というルールを設定しておく。これにより、通常の原稿と区切り用紙との区別をすることができる。この場合、紙文書としてスキャンしたい原稿中に、区切り用紙の条件を満たしてしまうものがあると、区切り用紙として誤認識されてしまうケースが考えられるので、区切り用紙の判定条件を複数用意しておき、ユーザがどの区切り用紙を使用するのか、情報表示・入力手段２２によって選択できるようにしておくことが好適である。

【0049】

ｃ）その他、紙文書間の区切りを検出する方法はいかなる方法であってもよい。例えば、紙文書の欄外に、１つの紙文書の最初のページと最後のページを表す所定のマークを付し、スキャン手段が該マークを検出し判別することで、文書電子化装置が自動的に紙文書間の区切りを検出できる。また、紙文書の欄外に付されたページ番号を読み取ることで、紙文書間の区切りを検出してもよい。

【0050】

紙文書間の区切りの設定が終了し、スキャンの開始が指示されると情報表示・入力手段２２がスキャン手段２に、署名付きスキャン要求を行う（Ｓ２）。スキャン手段２は、紙文書１の第１ページからスキャンを開始し、上述した紙文書間の区切りまで（紙文書１のスキャンが終了するまで）スキャンを実行する（Ｓ３）。紙文書１のスキャンが終了したら、スキャン手段２はデータ保存手段２４に画像データを出力し（Ｓ４）、データ保存手段２４は紙文書１の画像データを記憶する（Ｓ５）。データ保存手段２４は、紙文書１の記憶が成功したら、成功を示す信号をスキャン手段２に出力する（Ｓ６）。

【0051】

紙文書１の画像データがデータ保存手段２４に記憶されたら、データ保存手段２４は、紙文書１の画像データのＭＤ１を生成する（Ｓ７）。以降は、ＡＤＦにセットされた全ての紙文書２～紙文書ｎのスキャンが終了するまでスキャンを実行し、画像データがデータ保存手段２４に記憶された画像データのＭＤ２～ＭＤｎが順次生成される（Ｓ８～Ｓ２３）。

【0052】

全ての紙文書のＭＤが生成されると、データ保存手段２４は、ＭＤ１～ＭＤｎを連結して、ＭＤ結合データ２９を作成する（Ｓ２４）。次いで、データ保存手段２４は、ＭＤ結合データ２９のＭＤ３０を生成する（Ｓ２５）。

【0053】

データ保存手段２４は、ＭＤ３０を機器署名手段４に出力し（Ｓ２６）、機器署名を要求する。機器署名手段４は、文書電子化装置が機器内に保持する暗号鍵（秘密鍵）を用いＭＤ３０を暗号化し、機器署名６を生成する（Ｓ２７）。機器署名手段４は、機器署名６をデータ保存手段２４に送信し（Ｓ２８）、データ保存手段２４は、機器署名６及びＭＤ結合データ２９を、各紙文書の各画像データに対応づけて、又は添付して、記憶する（Ｓ２９）。以上で、機器による電子署名（機器署名）が得られた。

【0054】

次いで、データ保存手段２４は、ＩＣカード８により責任者署名を行うために、情報表示・入力手段２２に、ＩＣカードの挿入を指示するメッセージを表示する（Ｓ３０）。ユーザによりＩＣカード８が挿入されると（Ｓ３１）、カード入出力手段２３が責任者署名手段７に、ＩＣカードが挿入されたことを通知する。なお、ＩＣカードが挿入された際に、ユーザ認証を行うことが好適である。責任者署名手段７は、ＩＣカードが挿入されたことをデータ保存手段２４に通知する（Ｓ３２）。

【0055】

次いで、データ保存手段２４は、責任者署名手段７にＭＤ３０を出力すると共に、電子署名を要求する（Ｓ３３）。責任者署名手段７は、ＭＤ３０を、カード入出力手段２３を介してＩＣカード８に送信する。ＩＣカード８は、ＭＤ３０を該ＩＣカードが保持する暗号鍵で暗号化して責任者署名９を生成し（Ｓ３４）、責任者署名機能７に送信する。責任者署名手段７は、責任者署名９をデータ保存手段２４に出力する（Ｓ３５）。データ保存手段２４は、責任者署名９を、各紙文書の各画像データに対応づけて、又は添付して、記憶する（Ｓ３６）。以上で、ＩＣカードによる電子署名（責任者署名）が得られた。

【0056】

データ保存手段２４は、機器署名６及び責任者署名９、並びに、ＭＤ結合データ２９が添付された画像データの配信を、保存データ配信手段２５に出力する（Ｓ３７）。保存データ配信手段２５は、配信要求のあった画像データを外部の記憶装置１１に配信する（Ｓ３８）。配信が終了すると保存データ配信手段２５は、配信が成功した旨の信号をデータ保存手段２４に出力する（Ｓ３９）。データ保存手段２４は、電子署名の付与が終了した旨のメッセージを情報表示・入力手段２２に表示する（Ｓ４０）。以上で、暗号処理に係る時間を低減させながら、複数の紙文書毎に検証可能な電子署名を付与する処理が終了した。

【0057】

本実施例によれば、複数の紙文書毎に検証可能な電子署名を、ＩＣカードによる暗号化処理の処理量を少なくして付与できるので、暗号化処理を高速に行うことができる。また、各紙文書が複数のページから構成されていても、各紙文書間の区切りを検出できるので、種々の紙文書をまとめて画像データに変換し、電子署名を付与できる。紙文書間の区切りは、ユーザが指示してもよいし、区切り用紙を使用してもよいし、また、紙文書の欄外のマークやページ番号を検出してもよいので、柔軟に紙文書間の区切りを検出できる。

【図面の簡単な説明】

【0058】

【図1】スキャンした紙文書に電子署名を付与する処理の流れを示す図である。

【図2】文書電子化装置の機能ブロック図である。

【図3】複数の紙文書に電子署名を付与する場合の紙文書とＭＤの関係を示す図である。

【図4】スキャンされた複数の紙文書に電子署名を付与する処理のシーケンス図である。

【図5】各紙文書のページ数を入力する表示画面の一例である。

【図6】紙文書間の区切りに区切り用紙を挟んだ複数の紙文書の一例である。

【符号の説明】

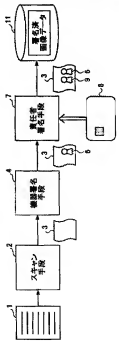
【0059】

１　紙文書
２　スキャン手段
３　画像データ

４　機器署名手段
６　機器署名
７　責任者署名手段
９　責任者署名
１０　プログラムを記録した記録媒体
１１　記憶装置
２２　情報表示・入力手段
２３　カード入出力手段
２４　データ保存手段
２５　保存データ配信手段
２９　ＭＤ結合データ
３０　ＭＤ結合データのＭＤ
３５　区切り用紙

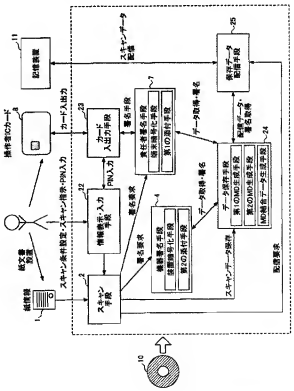
【図1】

スキャンした紙文書に電子署名を付与する処理の流れを示す図



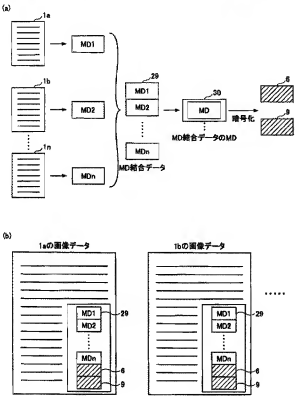
【図2】

紙文書電子署名装置の機能ブロック図



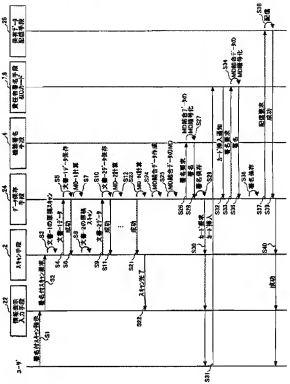
【図3】

複数の紙文書に電子署名を付与する場合の紙文書とMDの関係を示す図



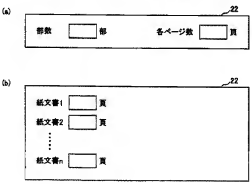
【図4】

スキャンされた複数の紙文書に電子署名を付与する処理のシーケンス図



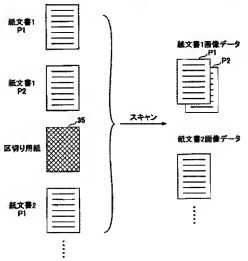
【図5】

各紙文書のページ数を入力する表示画面の一例



【図6】

紙文書間の区切りに区切り用紙を挟んだ複数の紙文書の一例



【要約の続き】
する。
【選択図】　図３